UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,412	12/21/2001	Alex J. Hinchliffe		3596

7590 07/21/2009

Zilka-Kotab PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
DENNISON, JERRY B	
ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/028,412	HINCHLIFFE ET AL.	
	Examiner	Art Unit	
	J Bret Dennison	2443	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5,7,9-16,18,19,21,23-30,32,33,35 and 37-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,7,9-16,18,19,21,23-30,32,33,35 and 37-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

RESPONSE TO AMENDMENT

1. This Action is in response to the Amendment for Application Number 10/028,412 received on 4/27/2009.

2. Claims 1-2, 4-5, 7 9-16, 18-19, 21, 23-30, 32-33, 35, 37-49 are presented for examination.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 4/27/2009 has been entered.

Claim Interpretation

4. Before a detailed rejection, a brief interpretation of peer-to-peer networks should be discussed. A peer-to-peer network is a communications network in which each party has the same capabilities and either party can initiate a communication session.

5. Peer-to-peer communication may be implemented in a client/server environment by giving each communication node, server and client, the same capabilities, meaning a client can be configured as a server and a server can be configured as a client. At any

given instant during transmission of a file, for instance, one computer is providing the file (server) and one computer is receiving the file (client).

6. To further support this interpretation, the Gnutella Protocol Specification v0.4 has been provided. The Gnutella Protocol Specification shows support that within a peer-to-peer network, every client is a server, and vice versa. These so-called Gnutella servents perform tasks normally associated with both clients and servers. They provide client-side interfaces through which users can issue queries and view search results, while at the same time they also accept queries from other servants, check for matches against their local data set, and respond with applicable results. Gnutella, being a well known peer-to-peer network, shows that a peer-to-peer network is simply comprised of clients and servers.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 11, 15, 16, 19, 25, 29, 30, 33, 39 and 45-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al. (U.S. Patent Number 5,862,335) in view of Meadway et al. (U.S. Patent Number 6,675,205).

1. Regarding claims 1, 15, and 29, Welch disclosed a computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity (Welch, col. 2, lines 35-43, Welch disclosed monitoring and analyzing logical connections and file transfers between stations within a computer network by determining the context of each packet in relationship to earlier packets exchanged between two stations. The stations may be user workstations within the computer network. User workstations sharing data with each other are also known as peers; col. 5, lines 55-67 Welch disclosed monitoring the file transfer between peer A and peer B. Therefore, Welch disclosed monitoring peers in a peer-to-peer network).

However, Welch did not explicitly state performing an action associated with a suspicious pattern of activity when the suspicious pattern of activity is detected in the peer-to-peer network; and

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network,

wherein the suspicious pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data;

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline.

In an analogous art, Meadway disclosed a peer-to-peer system in which a central site directs peer systems to each other for file sharing (Meadway, col. 1, lines 45-52), providing a way for peers to directly transfer the requested file without the need of the server (Meadway, col. 1, lines 63-65), with indexing occurring on the peer to monitor the changes made to the files that the peer is sharing, with the updates transmitted to the central service (Meadway, col. 2, lines 1-10),

performing an action associated with a suspicious pattern of activity when the suspicious pattern of activity is detected in the peer-to-peer network (Meadway, col. 4, lines 18-25, Meadway disclosed when the central server receives an updated version of the client's index of shared data, the central server performs updating the central server's local index); and

wherein the peer-to-peer network permits peers to connect and operate substantially without a server by utilizing the server, at most, for providing addresses for the peers in the peer-to-peer network (Meadway, col. 1, lines 63-65, Meadway disclosed providing a way for peers to directly transfer the requested file without the need of the server);

wherein the suspicious pattern of activity is defined in terms of a configuration of shared data on a peer, the configuration establishing a baseline of authorized shares and permissions in association with the shared data (Meadway, col. 2, lines 35-40, col. 4, lines 18-25, Meadway disclosed the agent at the client reporting to the central server the identities of files on the computer that will be provided if requested by others, and when an update occurs to this shared data, the central server is notified, and the central

server updates its local index, the update to the shared data being authorized by the client, and permitted by the client to be shared, the baseline being either the index of the client, or the local index of the central server, since both contain data that is updated in association with the shared data of the client).

wherein monitoring a peer-to-peer network comprises evaluating a change with respect to the shared data on a peer in the peer-to-peer network, the change being made with respect to the baseline (Meadway, col. 4, lines 18-25, Meadway disclosed evaluating a change in the client's index of shared data, and updating the central server's local index).

Welch provides the monitoring of file transfers and logical connections to diagnose problems encountered within the network (Welch, col. 1, lines 34-35) in order to determine exchange of data as well as which application programs are being used (Welch, col. 1, lines 43-45).

Meadway provides indexing the identities of files located at each peer in which the peer is sharing (Meadway, col. 2, lines 6-10, 35-40). The teachings of Meadway enhances the diagnostics of Welch by providing the management system with not only exchange of data, but also the contents of the data to be exchanged (Meadway, col. 1, lines 65-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Meadway into Welch to provide the management system of Welch with more information regarding the file transfers, by providing indexes of the contents of files that peers of the network are

allowing to be shared (Meadway, col. 2, lines 10-20) in order to provide an enhanced system to diagnose problems (Welch, col. 1, lines 34-35) encountered in the computer network.

Claims 15 and 29 include a computer-readable medium and system performing the same functionality as claim 1. Both Welch and Meadway disclosed a computer-readable medium and system (Welch, Fig. 1; Meadway, Fig. 3). Therefore claims 15 and 29 are rejected under the same rationale.

2. Regarding claims 2, 16, and 30, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein monitoring a peer-to-peer network comprises:

evaluating network traffic among peers in the peer-to-peer network (Welch, col. 3, lines 25-30).

3. Regarding claims 5, 19, and 33, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol (Welch, col. 3, lines 25-30, 45-50).

4. Regarding claims 11, 25, and 39, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the

patterns of activity are local to a peer in the peer-to-peer network (Welch, col. 10, lines 5-10).

5. Regarding claim 45, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a share configuration loop is executed to detect changes to shares and corresponding permissions, and take action as a function of a type of the changes (Meadway, col. 2, lines 1-10).

6. Regarding claim 46, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claim 45 including wherein the share configuration loop is executed dynamically (Meadway, col. 2, lines 1-10).

7. Regarding claim 47, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claim 45 including wherein the share configuration loop is executed on a schedule (Meadway, col. 2, lines 1-10).

8. Regarding claim 48, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claim 45 including wherein the share configuration loop examines a current share configuration against a previously recorded share configuration (Meadway, col. 2, lines 1-10).

9. Regarding claim 49, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claim 45 including wherein, if the change includes an attempt to un-share a file or directory the action includes a log entry (Meadway, col. 2, lines 1-10, 35-41).

Claims 4, 7, 9, 10, 12-14, 18, 21, 23, 24, 26-28, 32, 35, 37,38, and 40-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al. (U.S. Patent Number 5,862,335) in view of Meadway et al. (U.S. Patent Number 6,675,205) as applied to claims 1, 15, and 29 above, and further in view of Conklin et al. (U.S. 5,991,881).

10. Regarding claims 4, 18, and 32, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.

In an analogous art, Conklin disclosed a network surveillance system that includes checking patterns of activity in comparison to a series of predefined or learned patterns which are pre-stored or developed from data received from the network (Conklin, col. 4 line 45 through col. 5, line10).

Welch and Meadway together provide a system of monitoring peers and their activity in a peer-to-peer network. The teachings of Welch and Meadway suggest peer-

to-peer networks that communicate using Transmission Control Protocol/Internet Protocol (Welch, col. 3, lines 45-67, Meadway, col. 3, lines 20-25).

The teachings of Conklin provide a network surveillance designed and intended to operate compatibly on networks which communicate using the Transmission Control Protocol/Internet Protocol, TCP/IP (Conklin, col. 2, lines 60-67).

Therefore, it would have been obvious to one in the ordinary skill in the art at the time of the invention to incorporate the teachings of Conklin into the teachings of Welch and Meadway to identify unauthorized activities such as methods and systems used by hackers to intrude into the peer-to-peer network (Conklin, col. 1, lines 10-15).

11. Regarding claims 7, 21, and 35, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address. In an analogous art, Conklin disclosed an intrusion detection function which identifies the network traffic as reportable activity when a packet matches a predefined intrusion profile indicating source and destination of the packet (Conklin, col. 5, lines 25-35). See motivation above.

12. Regarding claims 9, 23, and 37, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state wherein the action comprises logging information about the particular

pattern. In an analogous art, Conklin disclosed keeping a log file about the patterns of activity (Conklin, col. 5, lines 33-35). See motivation above.

13. Regarding claims 10, 24, and 38, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state wherein the action comprises sending an alert about the particular pattern. In an analogous art, Conklin disclosed sending out an alert when a pattern is detected (Conklin, col. 5, lines 30-33). See motivation above.

14. Regarding claims 12, 26, and 40, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state wherein the patterns of activity are global to the peer-to-peer network. In an analogous art, Conklin disclosed the network surveillance system capturing traffic that is broadcast (Conklin, col. 2, lines 50-58). See motivation above.

15. Regarding claims 13, 27, and 43, Welch and Meadway disclosed the limitations, substantially as claimed, as described in claims 1, 15, and 29. Welch and Meadway did not explicitly state obtaining a set of rules specifying the patterns of activity and associated actions. In an analogous art, Conklin disclosed obtaining pre-stored patterns of activity in a database (Conklin, col. 4, lines 45-55). See motivation above.

16. Regarding claims 14, 28, and 44, Welch, Meadway, and Conklin disclosed the limitations, substantially as claimed, as described in claims 13, 27, and 43, including refreshing the set of rules when the set of rules changes (Conklin, col. 4, lines 48-52).

17. Regarding claim 41, Welch, Meadway, and Conklin disclosed the limitations, substantially as claimed, as described in claim 40, including wherein the system is a border firewall (Conklin, col. 4, lines 45-55).

18. Regarding claim 42, Welch, Meadway, and Conklin disclosed the limitations, substantially as claimed, as described in claim 40, including wherein the system is a domain name server (Meadway, col. 3, lines 20-25).

Response to Amendment

Applicant's arguments and amendments filed on 4/27/2009 have been carefully considered but they are not deemed fully persuasive.

As detailed in the Board Decision filed on 2/26/2009, Appellants have not supported their argument with a definition of "suspicious activity" that precludes that term from being read on Meadway's index update information [Board Decision, 17]. It is noted that while the claim now recites a "suspicious pattern of activity", the Appellants still have not supported their argument with a definition of such that precludes this phrase from being read on Meadway's index update information.

It is the Examiner's position that Applicant has not yet submitted claims drawn to limitations, which define the operation and apparatus of Applicant's disclosed invention in manner, which distinguishes over the prior art.

Failure for Applicant to significantly narrow definition/scope of the claims and supply arguments commensurate in scope with the claims implies the Applicant intends broad interpretation be given to the claims. The Examiner has interpreted the claims with scope parallel to the Applicant in the response and reiterates the need for the Applicant to more clearly and distinctly define the claimed invention.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to J. Bret Dennison whose telephone number is (571) 272-3910. The examiner can normally be reached on M-F 8:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/J Bret Dennison/
Primary Examiner, Art Unit 2443